The General Data Protection Regulation (GDPR)

On the 25th of May 2018, a European privacy law, known as the General Data Protection Regulation (GDPR) will go into effect. The law imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyse data tied to EU residents. The GDPR applies no matter where you are located.

Who is affected? Some definitions

GDPR makes a clear distinction between the Data Controller and the Data Processor.

"Controller – means the natural or legal entity, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data...". From the point of view of Exelsys HCM this is the customer who is using Exelsys.

"Processor - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.". From the point of view of Exelsys this is Exelsys.

What are the requirements?

The GDPR contains many requirements about how you collect, store and use personal information. This means not only how you identify and secure the personal data in your systems, but also how you accommodate new transparency requirements, how you detect and report personal data breaches, and how you train privacy personnel and employees.

Where does Exelsys stand with regards to the GDPR requirements that relate to Data Processors?

Exelsys has been designed with data security and privacy in mind and a lot of the GDPR requirements are already covered. The transfer of all our platforms to Windows Azure PaaS, at the beginning of this year has further increased our compliance with GDPR. Windows Azure from Microsoft offers the most comprehensive set of compliance capabilities of any cloud service provider, leading the industry in engaging with customers, regulatory bodies, and standards boards to advance compliance and serve customers' needs. Microsoft designed Azure with industry-leading security measures and privacy policies to safeguard your data in the cloud, including the categories of personal data identified by the GDPR. Exelsys can help you on your journey to reducing risks and achieving compliance with the GDPR.

Specifically, Exelsys already fully addresses most of the requirements for Processors as listed below:

1) Appointment of sub-processors (Art.28(2), (4)): Exelsys does not use sub-processors.
2) Processor's obligation of confidentiality (Art.28(3)(b), 29): Fully covered by the existing Exelsys Online Services Agreement.
3) Compliance with the controller's instructions (Art.29): Exelsys, as per the Online Agreement and Terms of Use, will not deal with customer data unless specifically requested in writing by the customer.
4) Records of processing activities (Art. 30(2)): Exelsys keeps a detailed record, in the User Access Log, of all functions used for processing data by user.
5) Data Security (Art.28(1), (3)(e), (4), 32) - Processors must implement appropriate technical and organisational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access:
    a. Passwords are encrypted
    b. Passwords can be configured to be complex and users to be requested to frequently change passwords
    c. Data is encrypted in transit (using SSL certificates) and at rest in the data center

   d. Data redundancy is provided by maintaining an online replicated copy of the data in a geographically different location within the EU
   e. Regular backups are maintained and kept for 14 days
   f. Exelsys carries out regular security reviews and tests, such as penetration tests
6) Restrictions on Cross-Border Data Transfers to third countries (Art. 44): Exelsys does not transfer data outside of the EU.
7) Right to be forgotten (Art. 14): Exelsys provides the tools to delete all records of an employee or applicant.

At Exelsys we are continuing to work towards streamlining our operations, with a target of being fully compliant with the GDPR requirements applicable to data processors, by Q1 2018.

What do you need to do?

Your company acting as a Data Controller, will be subject to new requirements. For most companies, the new requirements will raise the bar above current privacy practices. Despite its complexity and new requirements, complying with the GDPR can be accomplished by following a structured approach.
You may wish to consider using the services of external consultants who specialise on the subject, to help you towards achieving GDPR compliance, or you can do it in-house if you have the necessary skills and competencies needed.

We recommend that you use a 5-step approach as follows:

1. Assemble the team and plan the process, create awareness
2. Analyse the current processes, identify gaps, assess the risks
3. Design and Implement
4. Review and Audit
5. Demonstrate On-going compliance

The above steps is only a suggestion, as each GDPR consultant is likely to implement a different approach.